

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-285026

(43)Date of publication of application : 13.10.2000

(51)Int.Cl. G06F 12/14  
G06F 12/00  
G09C 1/00  
H04L 9/32  
// G06F 17/30

(21)Application number : 11-093852

(71)Applicant : RICOH CO LTD

(22)Date of filing : 31.03.1999

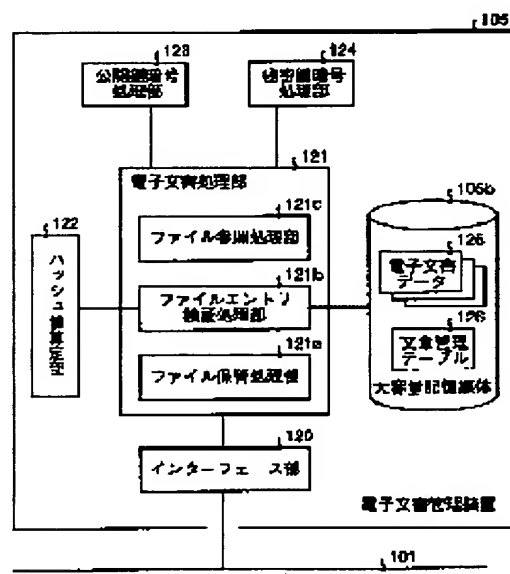
(72)Inventor : KANAI YOICHI

(54) ELECTRONIC DOCUMENT MANAGEMENT SYSTEM, ITS MANAGING METHOD AND COMPUTER READABLE RECORDING MEDIUM  
RECORDING PROGRAM FOR EXECUTING THE METHOD BY COMPUTER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an electronic(E) document management system capable of quickly outputting access permission to a legal user while efficiently preventing the generation of an unapproved access to an E document and the alteration of an E document, an E document managing method and a recording medium.

SOLUTION: In the case of storing an E document, a file storage processing part 121a calculates an entry signature by ciphering the hash value of a temporary file consisting of the file name of the E document, a document signature obtained by ciphering the document hash value of E document data by a private key and an access limitation list by the private key and stores a file entry to which the entry signature is added in a document management table 126 stored in a large capacity storage medium 105b.



## LEGAL STATUS

[Date of request for examination]

20.06.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-285026

(P2000-285026A)

(43) 公開日 平成12年10月13日 (2000. 10. 13)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
12/00	5 3 7	12/00	5 3 7 A 5 B 0 7 5
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 B 0 8 2
	6 6 0		6 6 0 D 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 1 9 A 0 0 1

審査請求 未請求 請求項の数11 O L (全 12 頁) 最終頁に続く

(21) 出願番号 特願平11-93852

(22) 出願日 平成11年3月31日 (1999. 3. 31)

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72) 発明者 金井 洋一

東京都大田区中馬込1丁目3番6号 株式会社リコー内

(74) 代理人 100089118

弁理士 酒井 宏明

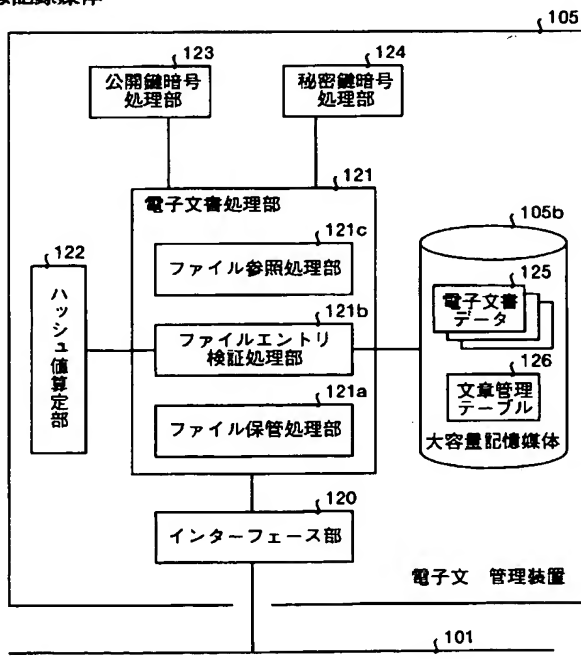
最終頁に続く

(54) 【発明の名称】 電子文書管理システム、電子文書管理方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 電子文書に対する許可なきアクセスや電子文書の改ざんを効率良く防止しつつ、正当なユーザに対するアクセス許可を迅速におこなうことができる電子文書管理システム、電子文書管理方法および記録媒体を提供すること。

【解決手段】 ファイル保管処理部121aが電子文書を保管する際に、電子文書のファイル名と、電子文書データの文書ハッシュ値をプライベートキーで暗号化した文書署名と、アクセス制限リストとからなる仮ファイルエントリのハッシュ値をプライベートキーで暗号化したエントリ署名を算定し、このエントリ署名を追加したファイルエントリを大容量記憶媒体105bの文書管理テーブル126に保管する。



BEST AVAILABLE COPY

## 【特許請求の範囲】

【請求項 1】 電子文書を送信するクライアントと、前記クライアントから受信した電子文書を暗号化して記憶部に保管するとともに、該記憶部に保管した電子文書へのアクセスを所定のアクセス制限リストに基づいて制限する電子文書管理装置とをネットワークを介して接続した電子文書管理システムにおいて、

前記文書管理装置は、

公開鍵暗号の秘密鍵を用いて前記クライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得する電子署名取得手段と、

前記電子署名取得手段が取得した電子署名および前記アクセス制限リストをその一部に含むファイルエントリを前記電子文書とともに前記記憶部に保管する保管手段と、

前記記憶部に保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を前記秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証する正当性検証手段とを備えたことを特徴とする電子文書管理システム。

【請求項 2】 前記保管手段は、前記電子文書に付与されたアクセス制限リストおよび前記電子署名を含むデータを前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得するエントリ署名取得手段と、前記エントリ署名取得手段が取得したエントリ署名を前記ファイルエントリに追加する追加手段とを備え、前記正当性検証手段は、前記記憶部に保管した電子文書をアクセスする際に、前記エントリ署名を前記公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出する改ざん検出手段を備えたことを特徴とする請求項 1 に記載の電子文書管理システム。

【請求項 3】 前記電子文書管理装置は、前記電子文書を乱数を用いて暗号化する電子文書暗号化手段と、前記電子文書暗号化手段が用いた乱数を前記公開鍵を用いて暗号化して暗号化乱数を生成する暗号化乱数生成手段と、前記暗号化乱数生成手段が生成した暗号化乱数を前記ファイルエントリに登録するとともに、前記電子文書暗号化手段が暗号化した電子文書を前記記憶部に格納する電子文書制御手段とをさらに備え、前記正当性検証手段は、前記電子文書および前記ファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を前記秘密鍵を用いて復号化して前記乱数を取得する乱数取得手段と、前記乱数取得手段が取得した乱数を用いて前記暗号化された電子文書を復号する電子文書復号手段とを備えたことを特徴とする請求項 1 または 2 に記載の電子文書管理システム。

【請求項 4】 前記電子署名取得手段は、前記クライアントから受信した電子文書の文書ハッシュ値を算定する文書ハッシュ値算定手段と、前記文書ハッシュ値算定手

段が算定した文書ハッシュ値を前記公開鍵暗号の秘密鍵を用いて暗号化して前記電子文書の電子署名を算定する電子署名算定手段とを備えたことを特徴とする請求項 1、2 または 3 に記載の電子文書管理システム。

【請求項 5】 前記エントリ署名取得手段は、前記電子文書のファイル名、前記文書署名取得手段が取得した電子署名および前記アクセス制限リストからなるデータのエントリハッシュ値を算定するエントリハッシュ値算定手段と、前記エントリハッシュ値算定手段が算定したエントリハッシュ値を前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定するエントリ署名算定手段とを備えたことを特徴とする請求項 2、3 または 4 に記載の電子文書管理システム。

【請求項 6】 電子文書を送信するクライアントから受信した電子文書を暗号化して記憶部に保管し、該記憶部に保管した電子文書へのアクセスを所定のアクセス制限リストに基づいて制限する電子文書管理方法において、公開鍵暗号の秘密鍵を用いて前記クライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得する電子署名取得工程と、

前記電子署名取得工程で取得した電子署名および前記アクセス制限リストをその一部に含むファイルエントリを前記電子文書とともに前記記憶部に保管する保管工程と、

前記記憶部に保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を前記秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証する正当性検証工程とを含んだことを特徴とする電子文書管理方法。

【請求項 7】 前記保管工程は、前記電子文書に付与されたアクセス制限リストおよび前記電子署名を含むデータを前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得するエントリ署名取得工程と、前記エントリ署名取得工程で取得したエントリ署名を前記ファイルエントリに追加する追加工程とを備え、前記正当性検証工程は、前記記憶部に保管した電子文書をアクセスする際に、前記エントリ署名を前記公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出することを特徴とする請求項 6 に記載の電子文書管理方法。

【請求項 8】 前記電子文書を乱数を用いて暗号化する電子文書暗号化工程と、前記電子文書暗号化工程で用いた乱数を前記公開鍵を用いて暗号化して暗号化乱数を生成する暗号化乱数生成工程と、前記暗号化乱数生成工程で生成した暗号化乱数を前記ファイルエントリに登録するとともに、前記電子文書暗号化工程で暗号化した電子文書を前記記憶部に格納する格納工程とをさらに備え、前記正当性検証工程は、前記電子文書および前記ファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を前記秘密鍵を用いて復

号化して前記乱数を取得する乱数取得工程と、前記乱数取得工程で取得した乱数を用いて前記暗号化された電子文書を復号する電子文書復号工程とを含んだことを特徴とする請求項6または7に記載の電子文書管理方法。

【請求項9】 前記電子署名取得工程は、前記クライアントから受信した電子文書の文書ハッシュ値を算定する文書ハッシュ値算定工程と、前記文書ハッシュ値算定工程で算定した文書ハッシュ値を前記公開鍵暗号の秘密鍵を用いて暗号化して前記電子文書の電子署名を算定する電子署名算定工程とを含んだことを特徴とする請求項6、7または8に記載の電子文書管理方法。

【請求項10】 前記エントリ署名取得工程は、前記電子文書のファイル名、前記文書署名取得工程で取得した電子署名および前記アクセス制限リストからなるデータのエントリハッシュ値を算定するエントリハッシュ値算定工程と、前記エントリハッシュ値算定工程で算定したエントリハッシュ値を前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定するエントリ署名算定工程とを含んだことを特徴とする請求項7、8または9に記載の電子文書管理方法。

【請求項11】 前記請求項6～10のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、電子文書を送信するクライアントから受信した電子文書を暗号化して記憶部に保管し、該記憶部に保管した電子文書へのアクセスを所定のアクセス制限リストに基づいて制限する電子文書管理システム、電子文書管理方法および記録媒体に関し、特に、電子文書に対する許可なきアクセスや電子文書の改ざんを効率良く防止しつつ、正当なユーザに対するアクセス許可を迅速におこなうことができる電子文書管理システム、電子文書管理方法および記録媒体に関する。

【0002】

【従来の技術】 従来、電子文書を管理する電子文書管理システムでは、システム内部に蓄積した電子文書のセキュリティの確保が重要な機能の一つとして位置づけられており、かかる電子文書は、明らかに不正なユーザだけではなくシステムを管理するシステム管理者であっても原則としてアクセスできるものであってはならない。

【0003】 すなわち、蓄積した電子文書のアクセス制御をおこなう場合には、通常はシステム管理者にアクセス特権を付与することが多いが、かかるシステム管理者は、あくまでもシステム自体を管理する管理者であって、電子文書の内容を管理する者ではないので、システム管理者といえども、全ての電子文書の内容を閲覧できる特権を与えるのは妥当ではない。

【0004】 このため、特開平9-218827号公報には、認証システム名とユーザ名とアクセス権とを設定したアクセス権リストを電子文書に付与して、この電子文書をアクセス権リストとともに暗号化する電子文書管理装置が開示されている。

【0005】

【発明が解決しようとする課題】 しかしながら、かかる従来技術では、本来秘匿する必要のないアクセス権リストを電子文書とともに暗号化するために、単にアクセス権の有無を調べる場合であっても、データ量の多い電子文書全体を復号化しなければならないために効率的ではない。

【0006】 特に、カラー画像データなどが挿入された電子文書を考えると、電子文書自体のデータ量が膨大なデータ量を有するため、アクセスの許可を確認する都度電子文書を復号することとすると、処理遅延が生じるために現実的ではない。

【0007】 このため、システム管理者をも含めた不正なユーザからの電子文書に対する許可なきアクセスや電子文書の改ざんを効率良く防止しつつ、正当なユーザに対するアクセス許可を迅速におこなうことができる電子文書管理システムをいかに実現するかが極めて重要な課題となっている。

【0008】 この発明は、上記問題（課題）に鑑みてなされたものであり、システム管理者をも含めた不正なユーザからの電子文書に対する許可なきアクセスや電子文書の改ざんを効率良く防止しつつ、正当なユーザに対するアクセス許可を迅速におこなうことができる電子文書管理システム、電子文書管理方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0009】

【課題を解決するための手段】 上記目的を達成するために、請求項1の発明に係る電子文書管理システムは、電子文書を送信するクライアントと、前記クライアントから受信した電子文書を暗号化して記憶部に保管するとともに、該記憶部に保管した電子文書へのアクセスを所定のアクセス制限リストに基づいて制限する電子文書管理装置とをネットワークを介して接続した電子文書管理システムにおいて、前記文書管理装置は、公開鍵暗号の秘密鍵を用いて前記クライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得する電子署名取得手段と、前記電子署名取得手段が取得した電子署名および前記アクセス制限リストをその一部に含むファイルエントリを前記電子文書とともに前記記憶部に保管する保管手段と、前記記憶部に保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を前記秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証する正当性検証手段とを備

えたことを特徴とする。

【0010】この請求項1の発明によれば、公開鍵暗号の秘密鍵を用いてクライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得し、取得した電子署名およびアクセス制限リストをその一部に含むファイルエントリを電子文書とともに記憶部に保管し、保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証することとしたので、記憶部に記憶された電子文書に対する不正な改ざんを検知することができる。

【0011】また、請求項2の発明に係る電子文書管理システムは、前記保管手段は、前記電子文書に付与されたアクセス制限リストおよび前記電子署名を含むデータを前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得するエントリ署名取得手段と、前記エントリ署名取得手段が取得したエントリ署名を前記ファイルエントリに追加する追加手段とを備え、前記正当性検証手段は、前記記憶部に保管した電子文書をアクセスする際に、前記エントリ署名を前記公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出する改ざん検出手段を備えたことを特徴とする。

【0012】この請求項2の発明によれば、電子文書に付与されたアクセス制限リストおよび電子署名を含むデータを秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得し、取得したエントリ署名をファイルエントリに追加し、記憶部に保管した電子文書をアクセスする際に、エントリ署名を公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出することとしたので、アクセス制限リストに不正な改ざんがなされた場合であっても、その改ざんを検知して電子文書に対する不正なアクセスを防止することができる。

【0013】また、請求項3の発明に係る電子文書管理システムは、前記電子文書管理装置は、前記電子文書を乱数を用いて暗号化する電子文書暗号化手段と、前記電子文書暗号化手段が用いた乱数を前記公開鍵を用いて暗号化して暗号化乱数を生成する暗号化乱数生成手段と、前記暗号化乱数生成手段が生成した暗号化乱数を前記ファイルエントリに登録するとともに、前記電子文書暗号化手段が暗号化した電子文書を前記記憶部に格納する電子文書制御手段とをさらに備え、前記正当性検証手段は、前記電子文書および前記ファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を前記秘密鍵を用いて復号化して前記乱数を取得する乱数取得手段と、前記乱数取得手段が取得した乱数を用いて前記暗号化された電子文書を復号する電子文書復号手段とを備えたことを特徴とする。

【0014】この請求項3の発明によれば、電子文書を

乱数を用いて暗号化し、この暗号化に用いた乱数を公開鍵を用いて暗号化して暗号化乱数を生成し、生成した暗号化乱数をファイルエントリに登録するとともに、暗号化した電子文書を記憶部に格納し、電子文書およびファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を秘密鍵を用いて復号化して乱数を取得し、取得した乱数を用いて暗号化された電子文書を復号することとしたので、不正ユーザによる電子文書の入手を防止することができる。

【0015】また、請求項4の発明に係る電子文書管理システムは、前記電子署名取得手段は、前記クライアントから受信した電子文書の文書ハッシュ値を算定する文書ハッシュ値算定手段と、前記文書ハッシュ値算定手段が算定した文書ハッシュ値を前記公開鍵暗号の秘密鍵を用いて暗号化して前記電子文書の電子署名を算定する電子署名算定手段とを備えたことを特徴とする。

【0016】この請求項4の発明によれば、クライアントから受信した電子文書の文書ハッシュ値を算定し、算定した文書ハッシュ値を公開鍵暗号の秘密鍵を用いて暗号化して電子文書の電子署名を算定することとしたので、文書ハッシュ値という指標を用いて電子文書の不正な改ざんを効率良く検知することができる。

【0017】また、請求項5の発明に係る電子文書管理システムは、前記エントリ署名取得手段は、前記電子文書のファイル名、前記文書署名取得手段が取得した電子署名および前記アクセス制限リストからなるデータのエントリハッシュ値を算定するエントリハッシュ値算定手段と、前記エントリハッシュ値算定手段が算定したエントリハッシュ値を前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定するエントリ署名算定手段とを備えたことを特徴とする。

【0018】この請求項5の発明によれば、電子文書のファイル名、電子署名およびアクセス制限リストからなるデータのエントリハッシュ値を算定し、算定したエントリハッシュ値を秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定することとしたので、エントリハッシュ値という指標を用いて効率良くアクセス制限リストの改ざんを検知することができる。

【0019】また、請求項6の発明に係る電子文書管理方法は、電子文書を送信するクライアントから受信した電子文書を暗号化して記憶部に保管し、該記憶部に保管した電子文書へのアクセスを所定のアクセス制限リストに基づいて制限する電子文書管理方法において、公開鍵暗号の秘密鍵を用いて前記クライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得する電子署名取得工程と、前記電子署名取得工程で取得した電子署名および前記アクセス制限リストをその一部に含むファイルエントリを前記電子文書とともに前記記憶部に保管する保管工程と、前記記憶部に保管した電子文書を

アクセスする際に、該電子文書のファイルエントリに含まれる電子署名を前記秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証する正当性検証工程とを含んだことを特徴とする。

【0020】この請求項6の発明によれば、公開鍵暗号の秘密鍵を用いてクライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得し、取得した電子署名およびアクセス制限リストをその一部に含むファイルエントリを電子文書とともに記憶部に保管し、保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証することとしたので、記憶部に記憶された電子文書に対する不正な改ざんを検知することができる。

【0021】また、請求項7の発明に係る電子文書管理方法は、前記保管工程は、前記電子文書に付与されたアクセス制限リストおよび前記電子署名を含むデータを前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得するエントリ署名取得工程と、前記エントリ署名取得工程で取得したエントリ署名を前記ファイルエントリに追加する追加工程とを備え、前記正当性検証工程は、前記記憶部に保管した電子文書をアクセスする際に、前記エントリ署名を前記公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出することを特徴とする。

【0022】この請求項7の発明によれば、電子文書に付与されたアクセス制限リストおよび電子署名を含むデータを秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得し、取得したエントリ署名をファイルエントリに追加し、記憶部に保管した電子文書をアクセスする際に、エントリ署名を公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出することとしたので、アクセス制限リストに不正な改ざんがなされた場合であっても、その改ざんを検知して電子文書に対する不正なアクセスを防止することができる。

【0023】また、請求項8の発明に係る電子文書管理方法は、前記電子文書を乱数を用いて暗号化する電子文書暗号化工程と、前記電子文書暗号化工程で用いた乱数を前記公開鍵を用いて暗号化して暗号化乱数を生成する暗号化乱数生成工程と、前記暗号化乱数生成工程で生成した暗号化乱数を前記ファイルエントリに登録するとともに、前記電子文書暗号化工程で暗号化した電子文書を前記記憶部に格納する格納工程とをさらに備え、前記正当性検証工程は、前記電子文書および前記ファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を前記秘密鍵を用いて復号化して前記乱数を取得する乱数取得工程と、前記乱数取得工程で取得した乱数を用いて前記暗号化された電子文書を

復号する電子文書復号工程とを含んだことを特徴とする。

【0024】この請求項8の発明によれば、電子文書を乱数を用いて暗号化し、この暗号化に用いた乱数を公開鍵を用いて暗号化して暗号化乱数を生成し、生成した暗号化乱数をファイルエントリに登録するとともに、暗号化した電子文書を記憶部に格納し、電子文書およびファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を秘密鍵を用いて復号化して乱数を取得し、取得した乱数を用いて暗号化された電子文書を復号することとしたので、不正ユーザによる電子文書の入手を防止することができる。

【0025】また、請求項9の発明に係る電子文書管理方法は、前記電子署名取得工程は、前記クライアントから受信した電子文書の文書ハッシュ値を算定する文書ハッシュ値算定工程と、前記文書ハッシュ値算定工程で算定した文書ハッシュ値を前記公開鍵暗号の秘密鍵を用いて暗号化して前記電子文書の電子署名を算定する電子署名算定工程とを含んだことを特徴とする。

【0026】この請求項9の発明によれば、クライアントから受信した電子文書の文書ハッシュ値を算定し、算定した文書ハッシュ値を公開鍵暗号の秘密鍵を用いて暗号化して電子文書の電子署名を算定することとしたので、文書ハッシュ値という指標を用いて電子文書の不正な改ざんを効率良く検知することができる。

【0027】また、請求項10の発明に係る電子文書管理方法は、前記エントリ署名取得工程は、前記電子文書のファイル名、前記文書署名取得工程で取得した電子署名および前記アクセス制限リストからなるデータのエントリハッシュ値を算定するエントリハッシュ値算定工程と、前記エントリハッシュ値算定工程で算定したエントリハッシュ値を前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定するエントリ署名算定工程とを含んだことを特徴とする。

【0028】この請求項10の発明によれば、電子文書のファイル名、電子署名およびアクセス制限リストからなるデータのエントリハッシュ値を算定し、算定したエントリハッシュ値を秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定することとしたので、エントリハッシュ値という指標を用いて効率良くアクセス制限リストの改ざんを検知することができる。

【0029】また、請求項11の発明に係る記録媒体は、前記請求項6～10のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項6～10の動作をコンピュータによって実現することができる。

【0030】

【発明の実施の形態】以下に添付図面を参照して、この

発明に係る電子文書管理システム、電子文書管理方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【0031】図2は、本実施の形態に係る電子文書管理システムの全体構成と電子文書管理装置のハードウェア構成とを示す図である。同図(a)に示すように、この電子文書管理システムは、クライアント102~104と、電子文書管理装置105とが、ネットワーク101に接続されたシステム構成となる。

【0032】クライアント102~104は、電子文書110を作成する文書処理機能と、作成した電子文書100の電子文書管理装置105への保管依頼機能と、電子文書管理装置105に保管した電子文書の参照および編集機能とを有する。

【0033】電子文書管理装置105は、クライアント102~104から保管依頼を受けた電子文書100を内部の大容量記憶媒体に保管する機能と、クライアント102~104の要求に応じて該当する電子文書100をクライアントに送信する機能とを有する。

【0034】ここで、この電子文書管理装置105は、クライアント102~104から受け付けた電子文書100の保管および取り出しを単におこなうのではなく、電子文書100自体の不正な改ざんや、電子文書100に対するアクセス制限を記述したアクセス制限リストの不正な改ざんを電子署名(デジタル署名)を用いて検出できるよう構成している。

【0035】また、この電子文書管理装置105では、電子文書100を平文で記憶するだけではなく、この電子文書100を暗号化して記憶することもできる。なお、かかる暗号化処理をおこなった場合には、正当なクライアントのみが電子文書100の正しい暗号鍵を入手できることとしている。

【0036】図2(b)に示すように、この電子文書管理装置105は、プロセッサ105aと、プログラム格納媒体105bと、大容量記憶媒体105cと、通信ポート105dとからなる。

【0037】プロセッサ105aは、プログラム格納媒体105bに格納した各種のプログラムを読み込んで、電子文書に係る各種処理を実行する処理部であり、プログラム格納媒体105bは、文書管理プログラム、ハッシュプログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを記憶する記憶部である。

【0038】ここで、この文書管理プログラムは、暗号化プログラムおよび復号化プログラムの処理に必要な公開鍵暗号系のプライベートキーを内在し、かかるプライベートキーは、外部からは読み出すことはできないものとする。

【0039】また、ここで言う暗号化プログラムおよび復号化プログラムには、電子文書を暗号化および復号化

するためのDES(Data Encryption Standard)暗号と、このDES暗号で用いる鍵や後述するハッシュ値を暗号化または復号化するための公開鍵暗号の両者が含まれる。

【0040】大容量記憶媒体105cは、ハードディスクドライブ(HDD)、CD-RまたはMOなどの書き換え可能な記録媒体からなる電子文書などを記憶する記憶部であり、通信ポート105dは、この電子文書装置105をネットワーク101に接続するための接続端子である。なお、ここでは説明の便宜上、この大容量記憶媒体105cをプログラム格納媒体105bと別個に設けた場合を示したが、両者を同じ記録媒体上に設けることもできる。

【0041】次に、本実施の形態に係る電子文書管理装置105の具体的な構成について説明する。図1は、本実施の形態に係る電子文書管理装置105の構成を示す機能ブロック図である。同図に示すように、この電子文書管理装置105は、インターフェース部120と、電子文書処理部121と、ハッシュ値算定部122と、公開鍵暗号処理部123と、秘密鍵暗号処理部124と、大容量記憶媒体105bとからなる。

【0042】インターフェース部120は、図2(b)に示す通信ポート105dおよびネットワーク101を介してクライアント102~104との間でデータ授受をおこなうネットワークインターフェースである。

【0043】電子文書処理部121は、クライアント102~104からネットワーク101を介して受け取った電子文書の保管や、クライアント102~104の要求に応じて電子文書の送信などをおこなう本装置の主体をなす処理部であり、ファイル保管処理部121aと、ファイルエントリ検証処理部121bと、ファイル参照処理部121cとを有する。

【0044】ここで、このファイル保管処理部121aは、クライアント102~104から受け取った電子文書を保管する処理部であり、具体的には、クライアント102~104から電子文書とともにこの電子文書を暗号化する旨を示すフラグを受け取ったならば、この電子文書を乱数で暗号化した電子文書データを作成し、暗号化しない旨のフラグを受け取った場合には、乱数による電子文書の暗号化はおこなわない。

【0045】また、このファイル保管処理部121aは、単に電子文書データを保管するだけではなく、保管する電子文書のファイルエントリを作成し、作成したファイルエントリを文書管理テーブル126に追加する処理をおこなう。

【0046】ここで、このファイルエントリは、電子文書のファイル名と、電子文書のハッシュ値をプライベートキーで暗号化した文書署名と、アクセス制限リストと、これらで形成される仮ファイルエントリのハッシュ値をプライベートキーで暗号化したエントリ署名と、電



子文書の暗号化に用いた乱数をパブリックキーで暗号化した暗号化乱数とからなる。

【0047】また、ファイルエントリ検証処理部121bは、ファイル保管処理部121aが文書管理テーブル126に追加したファイルエントリの検証をおこなう処理部である。さらに、ファイル参照処理部121cは、クライアント102～104の要求に応答して大容量記憶媒体105bに記憶した電子文書ファイルを参照する処理部である。

【0048】ハッシュ値算定部122は、電子文書処理部121の要求に応じて電子文書に対応するハッシュ値若しくは電子文書のファイル名、文書署名およびアクセス制限リストで形成される仮ファイルエントリに対応するハッシュ値を算定する処理部である。

【0049】公開鍵暗号処理部123は、電子文書自体を暗号化するためではなく、ハッシュ値に電子署名を施したり、電子文書の暗号化に用いた暗号鍵(乱数)を暗号化または復号化するために用いる暗号処理部である。なお、この公開鍵暗号処理部123では、RSA (Rivest-Shamir-Adleman) 暗号などを用いることになる。

【0050】秘密鍵暗号処理部124は、電子文書自体を暗号鍵(乱数)を用いて暗号化する場合に用いる暗号処理部であり、たとえば米国商務省標準局が公布したDES暗号(Data Encryption Standard)などを用いることができる。

【0051】次に、図1に示すファイル保管処理部121aによる電子文書の保管処理手順について具体的に説明する。図3は、このファイル保管処理部121aによる電子文書の保管処理の概念を示す概念図であり、図4は、このファイル保管処理部121aによる電子文書の保管処理手順を示すフローチャートである。なお、ここでは、電子文書のファイル名が「sample01.doc」であり、ファイルアクセス制限リストが、「user1 RW、user2 R、user3 R」である場合を示している。

【0052】図3に示すように、電子文書管理装置105がクライアント102～104から電子文書データ、電子文書のファイル名、アクセス制限リストおよび暗号化フラグを受け取ると、ファイル保管処理部121aは、電子文書データの文書ハッシュ値を算定した後(ステップS401)、この文書ハッシュ値をプライベートキーで暗号化して文書署名を取得する(ステップS402)。

【0053】その後、電子文書のファイル名「sample01.doc」、文書署名およびファイルアクセス制限リスト「user1 RW、user2 R、user3 R」からなる仮ファイルエントリを作成し(ステップS403)、仮ファイルエントリのエントリハッシュ値を算定し(ステップS404)、算定したエントリハッシュ値をプライベートキーで暗号化してエントリ署名を取得し(ステップS405)、取得したエントリ署名を仮ファイルエントリに追

加してファイルエントリを作成する(ステップS406)。

【0054】ここで、暗号化フラグにより暗号化が指定されている場合には(ステップS407肯定)、秘密鍵暗号処理用の乱数を発生して電子文書データを暗号化するとともに(ステップS408)、この暗号化に用いた乱数をパブリックキーで暗号化して暗号化乱数を取得して(ステップS409)、取得した暗号化乱数をファイルエントリに追加する(ステップS410)。なお、暗号化フラグにより暗号化が指定されていない場合には(ステップS407否定)、上記ステップS408～S410の処理はおこなわない。

【0055】その後、このファイルエントリを文書管理テーブル126に追加した後(ステップS411)、この文書管理テーブル126と必要に応じて暗号化した電子文書データを大容量記憶媒体105bに記録した後(ステップS412～S413)、作成したファイルエントリをクライアントに返して処理を終了する(ステップS414)。

【0056】上記一連の処理をおこなうことにより、電子文書データを大容量記憶媒体105bに保存する際に、暗号化されていないアクセス容易なアクセス制限リストと、電子文書の文書署名と、エントリ署名と、暗号化乱数とからなるファイルエントリを文書管理テーブル126に登録することができる。

【0057】なお、上記ファイルエントリをクライアントを返すこととしたのは、クライアントの指示に応答して電子文書が正しく保管されたか否かをパブリックキーを利用して検証できるようにするためである。

【0058】そこで、次に図1に示すファイルエントリ検証処理部121bによる処理手順について説明する。図5は、図1に示すファイルエントリ検証処理部121bの処理手順を示すフローチャートである。同図に示すように、このファイルエントリ検証処理部121bは、クライアントからファイルエントリの検証指示を受け付けたならば、このファイルエントリからエントリ署名を取得するとともに(ステップS501)、ファイル名、文書署名およびアクセス制御リストを取得する(ステップS502)。

【0059】そして、これらのデータから仮ファイルエントリを作成し(ステップS503)、作成した仮ファイルエントリのエントリハッシュ値を取得する(ステップS504)。また、ファイルエントリから取得したエントリ署名をパブリックキーで復号して検証ハッシュ値とし(ステップS505)、この検証ハッシュ値とエントリハッシュ値とを比較する(ステップS506)。

【0060】その結果、両者が一致する場合には(ステップS507肯定)、電子文書が正常に保管されたものと判定してその旨をクライアントに返送し(ステップS508)、両者が一致しない場合には(ステップS50



7否定)、電子文書が正常に保管されなかったものと判定してその旨をクライアントに返送する(ステップS509)。上記一連の処理をおこなうことにより、クライアントの要求に応じて電子文書が正常に保管されたか否かをパブリックキーに基づいて確認することができる。

【0061】次に、図1に示すファイル参照処理部121cによるファイル参照手順について説明する。図6は、図1に示すファイル参照処理部121cによるファイル参照手順を示すフローチャートである。同図に示すように、このファイル参照処理部121cは、大容量記憶媒体105bから文書管理テーブル126を読み出し(ステップS601)、読み出した文書管理テーブル126から該当する電子文書のファイルエントリを取得し(ステップS602)、このファイルエントリからアクセス制御リストを取得する(ステップS603)。

【0062】そして、図5を用いて説明したファイルエントリの検証処理を実行し(ステップS604)、ファイルエントリが正当なものであるか否かを確認する(ステップS605)。この場合には、図5のステップS508はファイルエントリが正当な場合に対応し、ステップS509はファイルエントリが正当でない場合に対応する。

【0063】そして、このファイルエントリが正当でないと判定された場合には(ステップS605否定)、エラー処理をおこない(ステップS610)、ファイルエントリが正当であると判定された場合には(ステップS605肯定)、ファイルエントリに暗号化乱数があるか否かを確認し(ステップS606)、暗号化乱数がある場合には(ステップS606肯定)、この暗号化乱数をプライベートキーで復号して乱数を取得し(ステップS607)、取得した乱数で電子文書ファイルを復号して電子文書データを取得し(ステップS608)、取得した電子文書データをクライアントに返送する(ステップS609)。これに対して、ファイルエントリに暗号化乱数がなければ(ステップS606否定)、そのまま電子文書データをクライアントに返送する(ステップS609)。

【0064】上記一連の処理をおこなうことにより、大容量記憶媒体105bに記憶した電子文書データ125や文書管理テーブル126のアクセス制御リストが改ざんされた場合に、その改ざんを検出することができる。

【0065】上述してきたように、本実施の形態では、ファイル保管処理部121aが電子文書を保管する際に、電子文書のファイル名と、電子文書データの文書ハッシュ値をプライベートキーで暗号化した文書署名と、アクセス制限リストとからなる仮ファイルエントリのハッシュ値をプライベートキーで暗号化したエントリ署名を算定し、このエントリ署名を追加したファイルエントリを大容量記憶媒体105bの文書管理テーブル126に保管するよう構成したので、電子文書データ125や

アクセス制限リストの改ざんを検知することができる。

【0066】また、暗号化を示す暗号フラグが指定された際に、秘密鍵暗号処理部124を用いて電子文書データを乱数で暗号化して電子文書データ125として保管するとともに、この乱数をパブリックキーで暗号化した暗号化乱数をファイルエントリに追加するよう構成したので、正当なクライアント以外が適正に復号化した電子文書データを取得することを防止することができる。

【0067】

【発明の効果】以上説明したように、請求項1の発明によれば、公開鍵暗号の秘密鍵を用いてクライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得し、取得した電子署名およびアクセス制限リストをその一部に含むファイルエントリを電子文書とともに記憶部に保管し、保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証するよう構成したので、記憶部に記憶された電子文書に対する不正な改ざんを検知することができる電子文書管理システムが得られるという効果を奏する。

【0068】また、請求項2の発明によれば、電子文書に付与されたアクセス制限リストおよび電子署名を含むデータを秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得し、取得したエントリ署名をファイルエントリに追加し、記憶部に保管した電子文書をアクセスする際に、エントリ署名を公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出するよう構成したので、アクセス制限リストに不正な改ざんがなされた場合であっても、その改ざんを検知して電子文書に対する不正なアクセスを防止することができる電子文書管理システムが得られるという効果を奏する。

【0069】また、請求項3の発明によれば、電子文書を乱数を用いて暗号化し、この暗号化に用いた乱数を公開鍵を用いて暗号化して暗号化乱数を生成し、生成した暗号化乱数をファイルエントリに登録するとともに、暗号化した電子文書を記憶部に格納し、電子文書およびファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を秘密鍵を用いて復号化して乱数を取得し、取得した乱数を用いて暗号化された電子文書を復号するよう構成したので、不正ユーザーによる電子文書の入手を防止することができる電子文書管理システムが得られるという効果を奏する。

【0070】また、請求項4の発明によれば、クライアントから受信した電子文書の文書ハッシュ値を算定し、算定した文書ハッシュ値を公開鍵暗号の秘密鍵を用いて暗号化して電子文書の電子署名を算定するよう構成したので、文書ハッシュ値という指標を用いて電子文書の不正な改ざんを効率良く検知することができる電子文書管

理システムが得られるという効果を奏する。

【0071】また、請求項5の発明によれば、電子文書のファイル名、電子署名およびアクセス制限リストからなるデータのエントリハッシュ値を算定し、算定したエントリハッシュ値を秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定するよう構成したので、エントリハッシュ値という指標を用いて効率良くアクセス制限リストの改ざんを検知することができる電子文書管理システムが得られるという効果を奏する。

【0072】また、請求項6の発明によれば、公開鍵暗号の秘密鍵を用いてクライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得し、取得した電子署名およびアクセス制限リストをその一部に含むファイルエントリを電子文書とともに記憶部に保管し、保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証するよう構成したので、記憶部に記憶された電子文書に対する不正な改ざんを検知することができる電子文書管理方法が得られるという効果を奏する。

【0073】また、請求項7の発明によれば、電子文書に付与されたアクセス制限リストおよび電子署名を含むデータを秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得し、取得したエントリ署名をファイルエントリに追加し、記憶部に保管した電子文書をアクセスする際に、エントリ署名を公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出するよう構成したので、アクセス制限リストに不正な改ざんがなされた場合であっても、その改ざんを検知して電子文書に対する不正なアクセスを防止することができる電子文書管理方法が得られるという効果を奏する。

【0074】また、請求項8の発明によれば、電子文書を乱数を用いて暗号化し、この暗号化に用いた乱数を公開鍵を用いて暗号化して暗号化乱数を生成し、生成した暗号化乱数をファイルエントリに登録するとともに、暗号化した電子文書を記憶部に格納し、電子文書およびファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を秘密鍵を用いて復号化して乱数を取得し、取得した乱数を用いて暗号化された電子文書を復号するよう構成したので、不正ユーザによる電子文書の入手を防止することができる電子文書管理方法が得られるという効果を奏する。

【0075】また、請求項9の発明によれば、クライアントから受信した電子文書の文書ハッシュ値を算定し、算定した文書ハッシュ値を公開鍵暗号の秘密鍵を用いて暗号化して電子文書の電子署名を算定するよう構成したので、文書ハッシュ値という指標を用いて電子文書の不正な改ざんを効率良く検知することができる電子文書管

理方法が得られるという効果を奏する。

【0076】また、請求項10の発明によれば、電子文書のファイル名、電子署名およびアクセス制限リストからなるデータのエントリハッシュ値を算定し、算定したエントリハッシュ値を秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定するよう構成したので、エントリハッシュ値という指標を用いて効率良くアクセス制限リストの改ざんを検知することができる電子文書管理方法が得られるという効果を奏する。

【0077】また、請求項11の発明に係る記録媒体は、前記請求項6～10のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項6～10の動作をコンピュータによって実現することができる。

【図面の簡単な説明】

【図1】この実施の形態に係る電子文書管理装置の構成を示す機能ブロック図である。

【図2】本実施の形態に係る電子文書管理システムの全体構成と電子文書管理装置のハードウェア構成とを示す図である。

【図3】図1に示すファイル保管処理部による電子文書の保管処理の概念を示す概念図である。

【図4】図1に示すファイル保管処理部による電子文書の保管処理手順を示すフローチャートである。

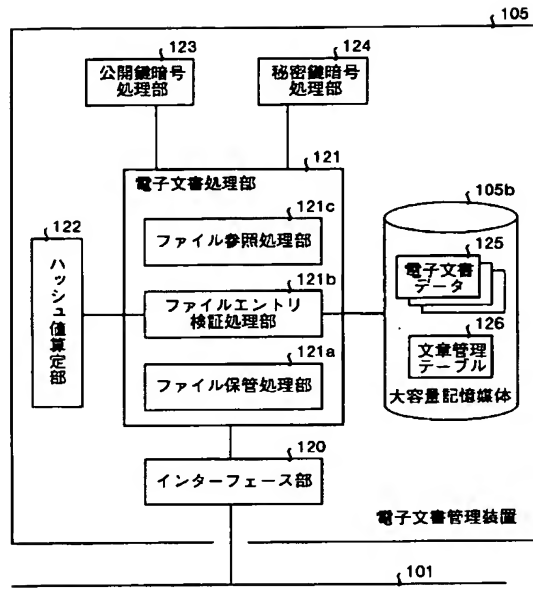
【図5】図1に示すファイルエントリ検証処理部の処理手順を示すフローチャートである。

【図6】図1に示すファイル参照処理部によるファイル参照手順を示すフローチャートである。

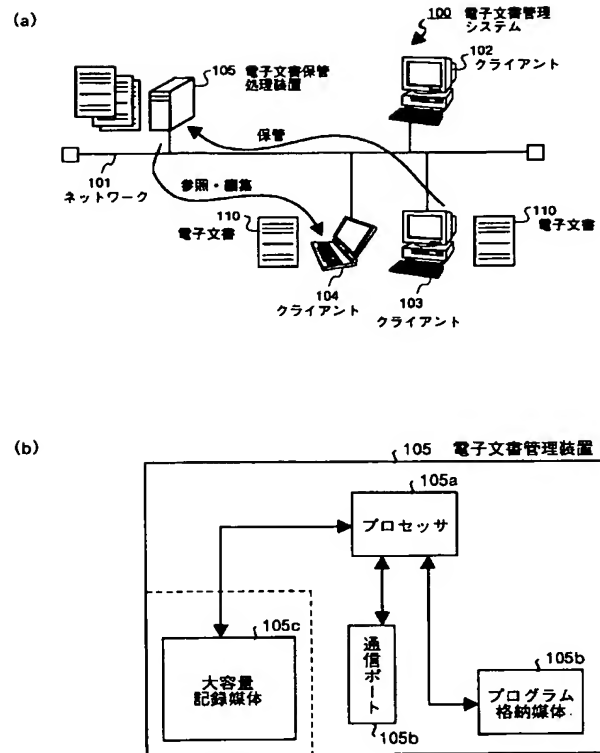
【符号の説明】

- 100 電子文書管理システム
- 101 ネットワーク
- 102, 103, 104 クライアント
- 105 電子文書管理装置
- 105a プロセッサ
- 105b プログラム格納媒体
- 105c 大容量記憶媒体
- 105d 通信ポート
- 120 インターフェース部
- 121 電子文書処理部
- 121a ファイル保管処理部
- 121b ファイルエントリ検証処理部
- 121c ファイル参照処理部
- 122 ハッシュ値算定部
- 123 公開鍵暗号処理部
- 124 秘密鍵暗号処理部
- 125 電子文書データ
- 126 文書管理テーブル

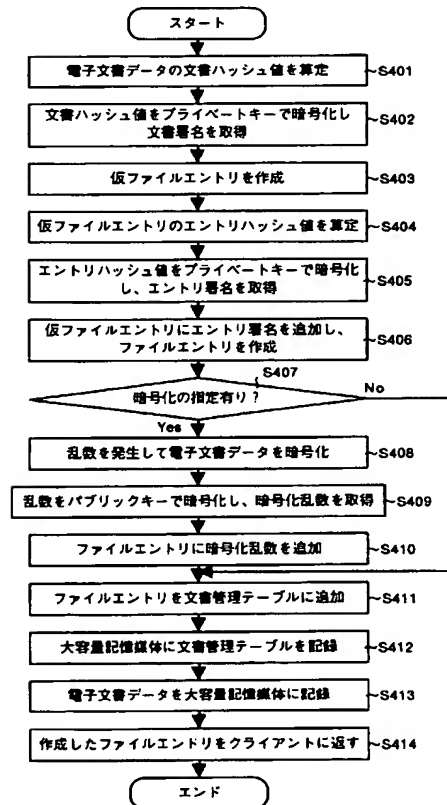
【図1】



【図2】

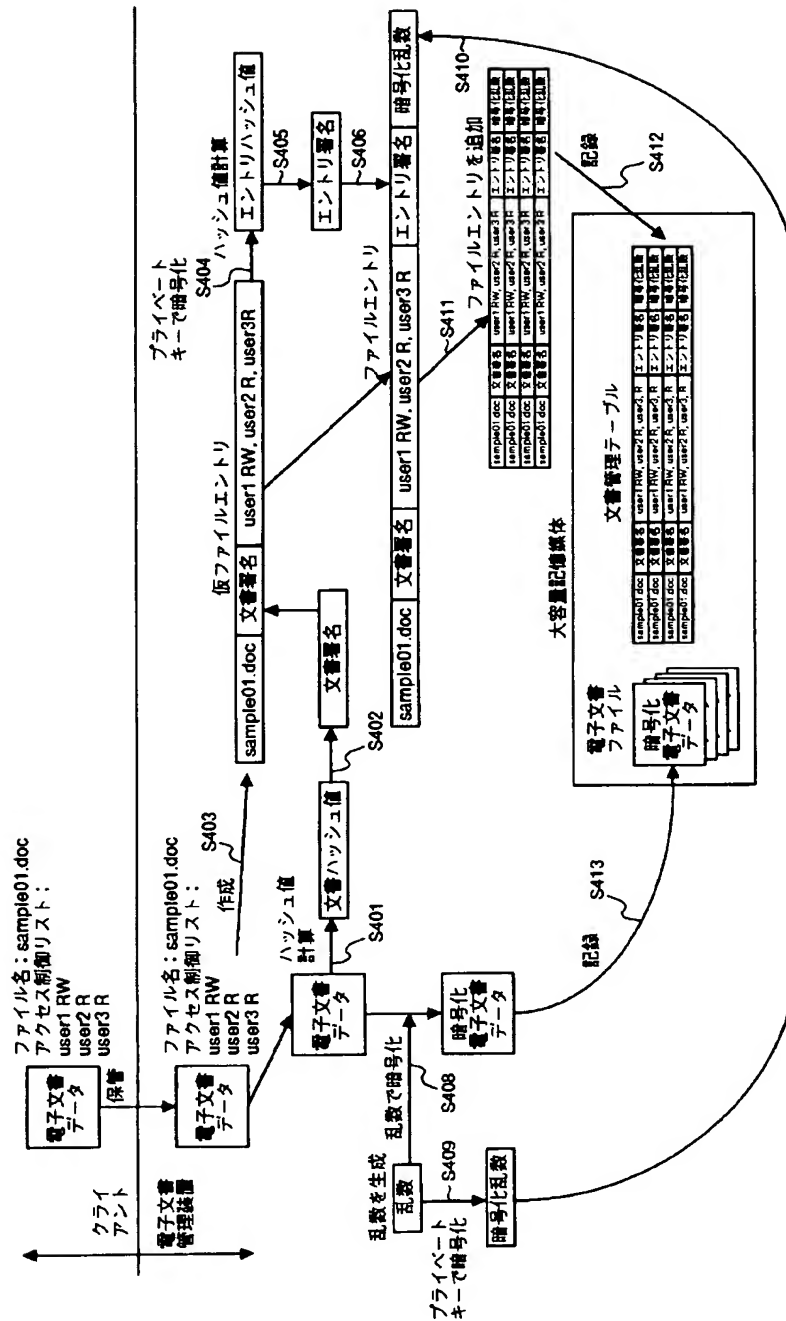


【図4】

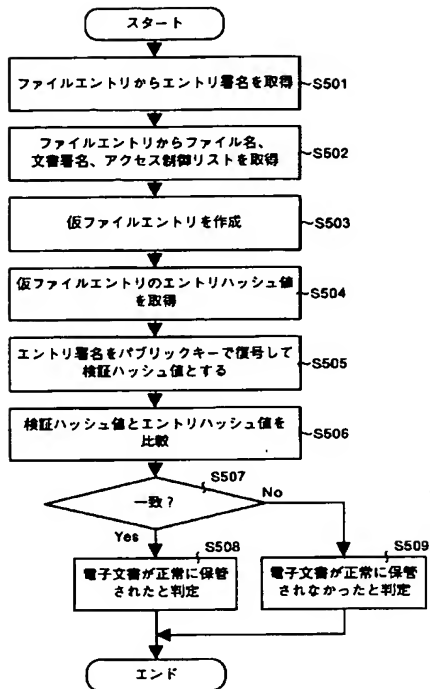


BEST AVAILABLE COPY

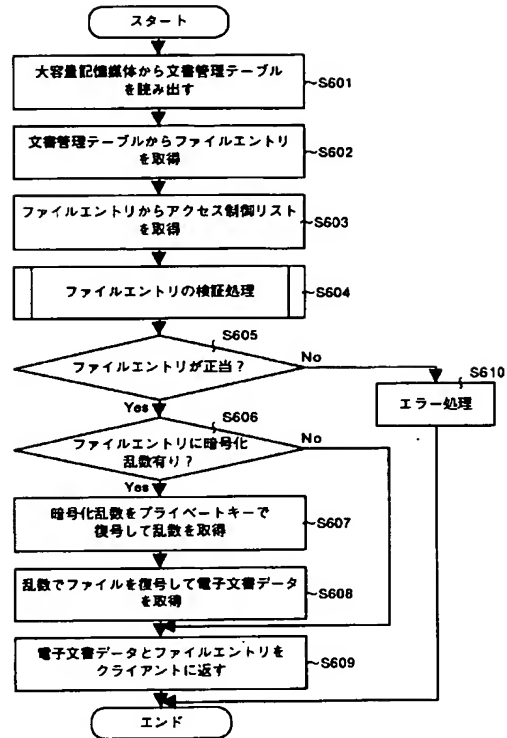
【図 3】



【図 5】



【図 6】



フロントページの続き

(51) Int. Cl.<sup>7</sup>

識別記号

// G 0 6 F 17/30

F I

テーマコード\* (参考)

H 0 4 L 9/00

6 7 5 B

G 0 6 F 15/40

3 2 0 B

F ターム (参考) 5B017 AA01 BA07 BB02 CA07 CA09  
CA165B075 KK43 KK54 KK60 KK63 NK45  
UU05

5B082 AA11 EA11 GA02 HA08

5J104 AA09 LA01 LA03 NA06 NA12  
NA38 PA07 PA149A001 BB03 BB04 CC02 EE02 EE03  
EE04 FF03 GG22 JJ13 LL03

BEST AVAILABLE COPY